Consultation response form

Please complete this form in full and return to IHconsultation@ofcom.org.uk

Consultation title	Protecting people from illegal harms online
Full name	Domestic Abuse Commissioner's Office
Contact phone number	
Representing (delete as appropriate)	Organisation
Organisation name	Domestic Abuse Commissioner's Office
Email address	Commissioner@domesticabusecommissioner.independent.gov.uk

Confidentiality

We ask for your contact details along with your response so that we can engage with you on this consultation. For further information about how Ofcom handles your personal information and your corresponding rights, see Ofcom's General Privacy Statement.

Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.	Nothing / Your name / Organisation name / Whole response / Part of the response (you will need to indicate which question responses are confidential)
Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.	None / Whole response / Part of the response (you will need to indicate below which question responses are confidential)
For confidential responses, can Ofcom publish a reference to the contents of your response?	Yes / No

Your response

Question (Volume 2)	Your response
Question 6.1: Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.	<u>General feedback on Volume 2:</u> In the Register of Risk, the onus is on users to demonstrate that behaviours/posts/actions online are harmful or how they impact women and girl. This makes the incorrect assumption that the online world is inherently neutral or safe. That starting point and that perspective is unhelpful, and I would suggest that the onus should be on platforms themselves to provide the evidence that their business models are safe and that they have inclusive policies. Platforms still don't have a taxonomy on types of harm related to misogyny and misogynoir. If platforms were recommended to do so, this could enhance the focus on safety by design and proactive measures rather than reactive, post-takedown culture. <u>Stalking, harassment and abuse</u> • There is a lack of information in this chapter on misogynistic algorithms supporting hateful content. More needs to be included to reflect the severity of the consequences of allowing these algorithms to be used. • I am happy to see that there is a recognition of perpetrators using multiple fake accounts and impersonating others. • There is currently no link detailed between a survivor's physical safety and the online world e.g., geo-tagging. There needs to be a better evidence base for this. • I would like to see an explicit link highlighted between harassment, stalking and domestic abuse. Most stalking cases will be in the context of domestic abuse - evidence suggests 50-60% overall[1] - and stalking is present in 94% of femicide cases[2] *but* this does not feature in the analysis. This means that the chapter misses the nuance and the potential risk of harm. • When it comes to stalking, risks look very different for domestic abuse victims and survivors than for someone who doesn't know their stalker. For example, if someone is stalking a celebrity, there is very little chance of that person being targeted in real life (although there is a very real psychological impact for victim), compared to partner stalking (or stalking by proxy) and making threats to rape/kill and the perpetrator following through with threats. Stalkers in a domestic context (intimate partner / ex-intimate partner) are a distinctive category in respect of prevalence, risk and attrition[3] and <u>must be treated as such in the guidance.</u>
Question 6.2: Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.	

[1] Modes of cyberstalking and cyberharassment: measuring the negative effects in the lives of victims in the UK (openrepository.com)
[2] 6896 Monckton-Smith (2019) Intimate Partner Femicide using Foucauldian.....pdf (glos.ac.uk)
[3] Stalking: Knowns and Unknowns - Lorraine Sheridan, Eric Blaauw, Graham Davies, 2003 (sagepub.com)

Question (Volume 2)	Your response
	• As mentioned in our ministerial letter, Ofcom do not discuss how online behaviour coexists with offline behaviour. Most stalking will be proximal[4], or cross-over (starts online, moves offline), not many stalkers stalk online only. There is no recognition of this. There is also no reference to physical / sexual abuse when Ofcom are highlighting impacts on victims – where perpetrators make threats, the evidence suggests 20-50% will follow through[5]. Ofcom mention the psychological impact of the threat, but not the fact that some perpetrators will go through with those threats which could be seen to minimise the abuse. • Tracking devices aren't addressed sufficiently in the guidance in terms of this chapter. When it comes to apps on phones, SMART technology and tech abuse, there are a wealth of concerns that need to be acknowledged and addressed. There should be a safety-proofing recommendation made for legitimate sites that harbour online illegal harms e.g., missing person sites where people can pay to try and find out where somebody is/what they are doing. These can be legitimate services used by landlords to track down missed rent, but this can also be misused for the stalking and harassment of victims and survivors. The outcome of this recommendation would be to make sure safety-by-design is built into these websites and that use with intent to cause harm is not possible. • I welcome the inclusion of guidance around services encouraging/facilitating suicide. However, there is a gap between stalking and harassment and this resulting in suicide and self-harm. Terms such as 'alarm' and 'distress' are frequently used, which undermines the potential severity of impact. • I would expect to see more links between individual stalking/harassment and the wider context of 'Incel' propaganda and content that informs and promotes the online social norms which perpetuate and encourage stalking, harassment and CCB. Lack of recognition of the risk and harm posed by misogynistic groups, such as the 'Incel' movement, stands to minimise the magnitude of the issue. • I wish to see more gender informed, specific language in this guidance (e.g., binary men or women) as stalking and harassment is highly prevalent in hate crime and homophobic crime. I am aware of (and welcome the fact that) the subsequent chapter uses more gender informed language. I do however believe strongly that it is important to highlight here also.

[4] Stalking: Knowns and Unknowns - Lorraine P. Sheridan, Eric Blaauw, Graham M. Davies, 2003 (sagepub.com)

[5] McEwan TE, Mullen PE, MacKenzie RD, Ogloff JR. Violence in stalking situations. Psychol Med. 2009 Sep;39(9):1469-78. doi: 10.1017/S0033291708004996. Epub 2009 Feb 12. PMID: 19215627.

Question (Volume 2)	Your response
	• I acknowledge that this Volume relates specifically to 'priority' illegal harms. However, it is important to name specific forms of other illegal harmful practices such as so-called honour-based abuse, female genital mutilation, and allied risks online (often mirroring offline harms as mentioned above.) • There seems to be a lack of acknowledgement that there is technology poverty in the BME community, widely experienced and evidenced during COVID[6]. It creates a discrepancy in victims' ability to access/afford safety features to counter online harm. • Moreover, women from BME and marginalised backgrounds can often face culturally specific forms of gender-based violence, which are exacerbated when carried out online and can have a hugely detrimental effect on the victim in their everyday life offline. It is important to be aware of these nuanced forms of abuse and that not every victim's life is impacted in the same way; what might be deemed a chauvinistic slur in some societies might hold greater weight in other places, to the extent that it could jeopardise the victim's character and cause them to be shamed, stigmatised, and ostracised from their wider community. • I am also disappointed that there is no recognition of the overlap between gendered abuse that targets women from faith backgrounds. Not only are women the biggest victims of hate crimes in the UK, but they are also subjected to some of the worst forms of online gendered violence that targets their faith identity. Women from these backgrounds are also subjected to gendered spiritual abuse, which takes place online and can have serious repercussions in their lives offline. • I am concerned by the focus on illegal content and how that impacts how course of conduct crimes such as stalking are dealt with. There is an acknowledgement that threatening content may not be illegal on its own (such as sending a picture of a front door), however I am still extremely concerned that content not deemed to be 'threatening' or 'abusive' will not be picked up. <u>Coercive and Controlling Behaviour (CCB)</u> • In codes of practice there is a small coverage of measures for CCB, e.g., block/mute functions, maybe not seeing suggested friends etc. However, this places the onus on the victim to respond to threat reactively and does not include sufficient proactive recommendations for mitigation. • CCB is an interaction of offline/online behaviour. This needs to be understood and reflected in the guidance.

[6] Exploring the impact of digital and data poverty on BAME people - Glitch UK

Question (Volume 2)	Your response
	• More needs to be included in this section around acts that interplay between CCB and harassment. Location tracking and the use of children to track/monitor/control victims needs to be highlighted as there is copious evidence of this[7]. This is double pronged in terms of the impact and harm on children and the victim. • Online theft of documents, paperwork etc. by perpetrator(s) as a form of CCB has not been addressed here. This would be useful in creating a more well-rounded and holistic picture of the harm - particularly digital passport information and immigration documents for migrant victims. <u>Intimate Image Abuse (IIA)</u> • It is important to acknowledge risk factors and multiple disadvantages for DA victims who are in sex work or are affected by trafficking linked offences[8]. We must also look to link risks with offline offences and allied risks such as spiking, blackmailing and gang-related offences. Without doing so, we cannot present a clear picture of harm and cannot advise services sufficiently in identifying and acting on risk factors. • 83% of women who had experienced threats to share their intimate images from a current or former partner experienced other forms of abuse, including over a quarter who experienced sexual abuse.[9] This interplay between IIA and other offences needs to be highlighted and to inform the recommendations in the guidance. Ofcom must recognise that the criminal justice system has not been set up to attend to incidents like these with the speed and accuracy required for the online world. We therefore must look to services to play this vital and necessary role in protecting victims and survivors from this abuse. <u>We therefore must extend the recommendation of hash-matching to intimate image abuse.</u> • Some open-source software – as opposed to AI tools such as Dall-E 3 or Midjourney, which have been trained to prohibit pornographic content – can currently be used to create anything users like, which can include realistic depictions of women and extreme and violent sexual fantasies. There are two points to make here. The first is that Ofcom should be

[7] PowerPoint Presentation (avaproject.org.uk); NSPCC (2023) The impact of coercive control on children and young people. Helplines insight briefing. London: NSPCC

[8] A Systematic Review of the Correlates of Violence Against Sex Workers - PMC (nih.gov)

[9] Refuge (2020) The Naked Threat. https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/~~onlinesafety/~~

Question (Volume 2)	Your response
	working with the tech industry (and creators of tools like Dall-E 3) to look at how services can be encouraged (or if necessary, obligated) to be 'safe by design'. The second is that big companies such as Google are contributing to traffic to these smaller services through their search and recommendation tools. We must ensure that these algorithms which facilitate and promote misogyny are highlighted and targeted in guidance.

Question (Volume 4 and 5)	Your response
General feedback on Volume 4 and 5	I am highly concerned that there doesn't seem to be any mention of stalking in Volume 5, which doesn't give any acknowledgement to how offences such as intimate image abuse interact with stalking cases. In previous conversations between the DAC office and Ofcom there was discussion of a helpline like that of 'Revenge Porn Helpline' for victims of DA related online abuse. This was a suggestion that DAC office was very supportive of. However, there is no clarity in this consultation about how victims would be supported and the specialise DA sector would be best placed to provide a solution to this problem. Will Ofcom support the setting up and running of a support service in the form of a helpline as mentioned in previous meetings?
	<u>Cost of Compliance:</u> There is an underlying assumption that tech companies will comply and will adopt best practise approaches. A key part of the rationale for introducing this legislation was a consensus among parliamentarians and civil society that self-regulation and relying on the voluntary initiative of tech companies to make the internet a safer place and to reduce harms was not working. The Online Harms White Paper highlights the patchwork of regulation and volunteer initiatives that had not gone far or fast enough. Nadine Dorries – Digital Secretary at the time - during second reading of the Bill highlighted that without the right incentives, tech companies will not do what is needed to protect their users. Claims about taking steps to fix issues via this assumption of compliance and best practice are not backed up by genuine actions. Systems that have been created for profit have a bottom line, and don't generally go the extra mile to ensure best practice, unless it is specifically part of their USP and a profit-driver. In other sectors, such as human rights, environmental rights and the financial sector - and specifically when thinking about the Online Safety Act -

Question (Volume 2)	Your response
	there is considerable evidence that platforms don't adhere to their own terms and conditions. For example, research that Refuge undertook last year interviewed survivors who reported illegal content to social media platforms. 53% said they didn't receive a response from a social media platform when they reported domestic abuse related content, and 95% said they weren't satisfied with the support received from social media companies. Platforms are not adhering to their terms and conditions currently and we therefore need to see a different approach to compliance. <u>Approaches to assessing illegal content:</u> It is important to define legal concept of illegal content. This description encapsulates the scope of the entire regime set out here. Duties are only linked and therefore applied to illegal content. In terms of human rights, the focus of most of the consultation currently centres around users and companies. There is not enough of a focus on the impacts on women's human rights. Ofcom's definition of illegal content seems to be based solely on criminal law without considering a systems approach to the actions of perpetrators. However, the Online Safety Act has been put in place to police a civil regime as well as a criminal one, and therefore Ofcom should not necessarily be looking solely for criminal thresholds to take action. Much of what this response has focused on around the broader impacts of harm will come to nothing if Ofcom do not consider a broader systems approach to priority offences. When balancing freedom of expression rights with recommending measures for strikes or blockings, Ocfom considers users mainly as 'speakers' and focuses on their rights in terms of freedom of expression. However, when thinking about the Human Rights Act, Ofcom fails to consider on balance the rights of users in terms of protection through blocking: "*although blocking and strikes may be a way of tackling illegal content, there are also concerns about the use of these systems on lawful speech"* It important to recognise that, while the 'takedown' approach that Ofcom has focused on will indeed assist individuals on case-by-case bases to take down content once it has already been posted, a better approach would be to think about the system in place. There can be better design choices being made by services and encouraged by Ofcom, and recommendations should be based more on design choices which perpetuate misogynistic/harmful behaviours with clear intent. The consultation should be focused on upstream safety by design, not reactive takedown measures.

Question (Volume 2)	Your response
	.

Please complete this form in full and return to IHconsultation@ofcom.org.uk.